ЗИРҲЛИ ҚАЛҚОН

ИЛМИЙ – АХБОРОТ ЖУРНАЛИ

№ 8 (20) 2022 йил декабрь

Мазкур журнал Чирчиқ олий танк қўмондонлик билим юртининг Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги ОАК Раёсатининг 2021 йил 4 июнь кунидаги № 300/5 қарорига асосан ҳарбий, педагогика, сиёсий ва тарих фанлари бўйича диссертациялар асосий натижаларини чоп этиш тавсия этилган илмий нашрлар рўйхатига киритилган илмий-ахборот журналидир.

Журналга Ўзбекистон Республикаси Мудофаа Вазирлиги раҳбарияти, ЎР ҚК Академияси, ЎР ҚК Ҳарбий Тиббиёт Академияси, МВ Ахборот Коммуникация Технологиялари ва Алоқа ҳарбий институти, ЎР Олий ҳарбий авиация билим юрти, Чирчиқ ОТҚМБЮ, ЎР ҚК кичик мутахассисларни тайёрлаш маркази ҳамда бошқа вазирлик ва идораларнинг олий таълим муассасалари профессор-ўқитувчилари, докторант, мустақил изланувчилари, тингловчилари, курсантлар ва қўшинлар офицерлари томонидан тайёрланган илмий мақолалари киритилган.

Журналдаги мақолаларда Қуролли Кучларнинг қурилиши ва ислох қилиниши, педогогика ва фандаги иннавацион ёндашувларнинг турли жиҳатлари ёритилади.

Журналдаги мақолалардан тўлиқ ёки қисман фойдаланилганда “Зирҳли қалқон” илмий-ахборот журналидан олинганлиги кўрсатилиши шарт.

Муаллиф фикри таҳририят нуқтаи назаридан фарқ қилиши мумкин. Мақолалардаги маълумотларнинг ҳаққонийлигига муаллифлар шахсан масъулдир.

“Зирҳли қалқон” илмий-ахборот журнали 2020 йил март ойидан чиқа бошлаган.

Журналда чоп этилган мақолалар бўйича таклиф ва мулоҳазаларни қуйидаги манзилга юборишингиз мумкин:
Индекс: 111715, Тошкент вилояти, Чирчиқ шаҳри Амир Темур кўчаси - 15, Чирчиқ ОТҚМБЮ.
Тел.: (+99870) 716-50-50. Факс: (+99870) 716-50-07. E-XAT: kanselyariya.chvtkiu@exat.uz.

МУНДАРИЖА

AXBOROT OQIMLARI TRAFIKLARINI BOSHQARISHNING NEYRO-NORAVSHAN MODELLARINI ISHLAB CHIQISH ASOSIDA TARMOQ TRAFIKLARNI ANOMAL BAHOLASH

IZBOSAROV A.F.,
Qurolli Kuchlari Bosh shtabi Aloqa, axborot texnologiyalari va axborotlarni himoyalash bosh boshqarmasi boshlig‘i, texnika fanlari doktori (DSc), O‘zbekiston Respublikasida xizmat ko‘rsatgan aloqa xodimi
NIGMATOV Z.Z.,
Chirchiq OTQMBYU Qo‘shinlar kundalik faoliyati va qo‘shinlarni boshqarish kafedrasi “Aloqa va axborot tizimlari” sikli o‘qituvchisi, texnika fanlari bo‘yicha falsafa doktori (PHD)
YAXYOYEV A.A.,
Telekommunikatsiya infratuzilmasini rivojlantirish bo‘limi boshlig‘i

Annotatsiya. Ushbu maqolada Mudofaa vazirligi telekommunikatsiya tarmoqlaridagi trafik anomaliyalarining holatlarni batafsil tasnifi ularning paydo bo‘lish sabablariga qarab keltirilgan, ya’ni tarmoq trafik anomallarni aniqlashning asosiy usullari batafsil bayon qilingan, jumladan ularning ishlash prinsiplari, shuningdek har birining afzalliklari va kamchiliklari bayon qilingan. Taqdim etilgan usullarning ichida anomal holatlarni bashorat qilish uchun eng samarali va maqbul usul statistik tahlildan foydalanadigan usul hisoblanadi, axborot oqimlarining tarmoq trafikning anomallari siklik tahlil asosida hisoblanadi. Bundan tashqari tarmoqdagi trafik anomallarni aniqlash uchun vositalar, xususan, hujumni aniqlash usulari keltirilgan. Tadqiqot obyekti etib - tarmoq trafikning anomaliyasi. Tadqiqot mavzusi Mudofaa vazirligi telekommunikatsiya tarmoqlarida axborot oqimlarining siklik tahlil orqali tarmoq trafik anomallarni baholash etib belgilandi.

Kalit so‘zlar: tarmoq trafigi, anomaliya, sikl tahlili, hisoblash tarmog‘i, neyron tizim, axborot xavfsizligi.

Maqolaning maqsadi - davriy tahlil asosida hisoblash tarmoq trafikining anomallarini baholash. Qo‘llanish sohasi - axborot-kommunikatsiya texnologiyalari. Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining anomallarni hisoblash uchun axboroti almashinuvini boshqarish metodologiyasi quyidagicha:

“tarmoq paketlari to‘g‘risida ma’lumot olish;
axborot oqimlarining prognozni tuzish;
anomallarni izlash va baholash;
anomaliyaga javob;
bazani to‘ldirish va tahrirlash” qoidalari.

Bundan tashqari, sikl tahlilini o‘tkazish metodologiyasi quyidagi bosqichlardan iborat:

“ma’lumotlarni tanlash;
ma’lumotlarni tekislash;
mumkin bo‘lgan sikllarni qidirish;
trafikdagi tendensiya tarkibiy qismlarini olib tashlash;
statistik ahamiyatga ega bo‘lgan sikllarni tekshirish;
"kelajakda" sikllarni birlashtirish va loyihalash.

Shunday qilib, vaqt ketma-ketligini tahlil qilish asosida taklif qilinadigan trafikni taxminiy algoritmi tarmoq trafigini davriy ravishda qidirish asosida tarmoqda axborotlar almashinuvida yuklamalar aniqlashga imkon beradi. Shuni ta’kidlash kerakki, axborotlar almashinuvida yuklamalarni prognozlashda tarmoqlaridagi trafik anomaliyalarining baholashning muhim tarkibiy qismi bo‘lib, tarmoq trafikining yuklamalar sonidan oshib ketishini boshqarish muammolarini tez va samarali hal qilishga imkon beradi.

Bugungi kunda zamonaviy axborot-kommunikatsiya tizimlarini keng joriy etish va Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining keskin oshib borishi va hisoblash tarmoqlari ma’lumotlarni qayta ishlash va uzatish uchun to‘liq funksional taqsimlangan hisoblash qurilmasi sifatida foydalanishni yangi usullari taklif qilinmoqda. Hozirgi vaqtda ma’lumotlarni uzatish texnologiyasining xarakterli xossalari va parametrlarini aniqlash.

Hisoblash tarmoqlarining ishlashida anomallarni aniqlashning maqbul kafolatlangan usullarini qidirish, unda qandaydir tarzda yuzaga keladigan jarayonlarga ta’sir qilishi mumkin bo‘lgan ko‘plab tadqiqotlar olib borilmoqda.

Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining va trafik tahlilini o‘rganish bugungi kunda juda muhimdir, chunki bunday tahlil hatto zararli dasturiy ta’minotlarining hujumini uning tayyorlanish bosqichida ham aniqlab berishi mumkin.

Maqolaning maqsadi tarmoq trafigida ushbu anomallarni aniqlash asosida Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining va trafikni boshqarish texnikasini ishlab chiqish orqali axborot-kommunikatsiya tizimlarida ma’lumotlarni uzatish samaradorligini oshirish. Ushbu maqsadga erishish uchun quyidagi vazifalarni hal qilish kerak:

1. Tarmoq trafigini bashorat qilishning mavjud usullarini tahlil qilish, ularning afzalliklari va kamchiliklarini aniqlash, vaqt ketma-ketligini tahlil qilish asosida trafikni bashorat qilishning matematik modelini ishlab chiqish.
2. Taklif etilgan model asosida Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining va tarmoq trafigini boshqarish metodologiyasini ishlab chiqish.
3. Integrallashgan boshqarish tizimlari tarmoq trafigidagi anomalliklarni identifikatsiyalash algoritmlarini ishlab chiqish
4. Metodologiya asosida anomaliya izlash va tarmoq trafigini boshqarish jarayonlarini rasmiylashtiradigan algoritmlarni ishlab chiqish, shuningdek algoritmlarga asoslanib, axborot oqimlarining boshqarish choralarini qo‘llash bo‘yicha qarorlarni qo‘llab-quvvatlash tizimini amalga oshiradigan dasturiy mahsulotni ishlab chiqish.

Kanallarning kengligi tez o‘sib borishi, shuningdek noma’lum hujumlar va zararli dasturlarning tez paydo bo‘lishi, o‘z o‘zidan zamonaviy hujumlarni aniqlash tizimlarning barchasi bugungi kunda uddasidan chiqaolmayapdi desak to‘g‘ri bo‘ladi. Buning sabablari quyidagilar deb olishimiz mumkin:

ko‘plab tizimlar ba’zi bir ajratilgan qurilmaga qaratilgan bo‘lib hujumlarni aniqlashga asoslangan (bunday tizimlar keng tarmoqlarga moslashtirilmagan);

Ko‘pincha aniqlash tizimlariga asoslangan usullar ma’lumotni tahlil qilishning imzo usulidan foydalanadilar, shu sababli noma’lum hujumlar o‘tkazib yuboriladi. [1]

Tarmoq hujumlarini va kompyuter tarmog‘ining ishlashiga ta’sir qiladigan zararli dasturlarni aniqlash usullaridan biri trafik anomallarini aniqlashdir.

Umumiy holatda anomaliya - bu normadan chetga chiqish yoki uzatilayotgan trafikdagi umumiy holat. Ushbu atama turli xil tarmoq hujumlariga, shu jumladan noma’lum hujumlarga (nolga teng hujum) tegishlidir.

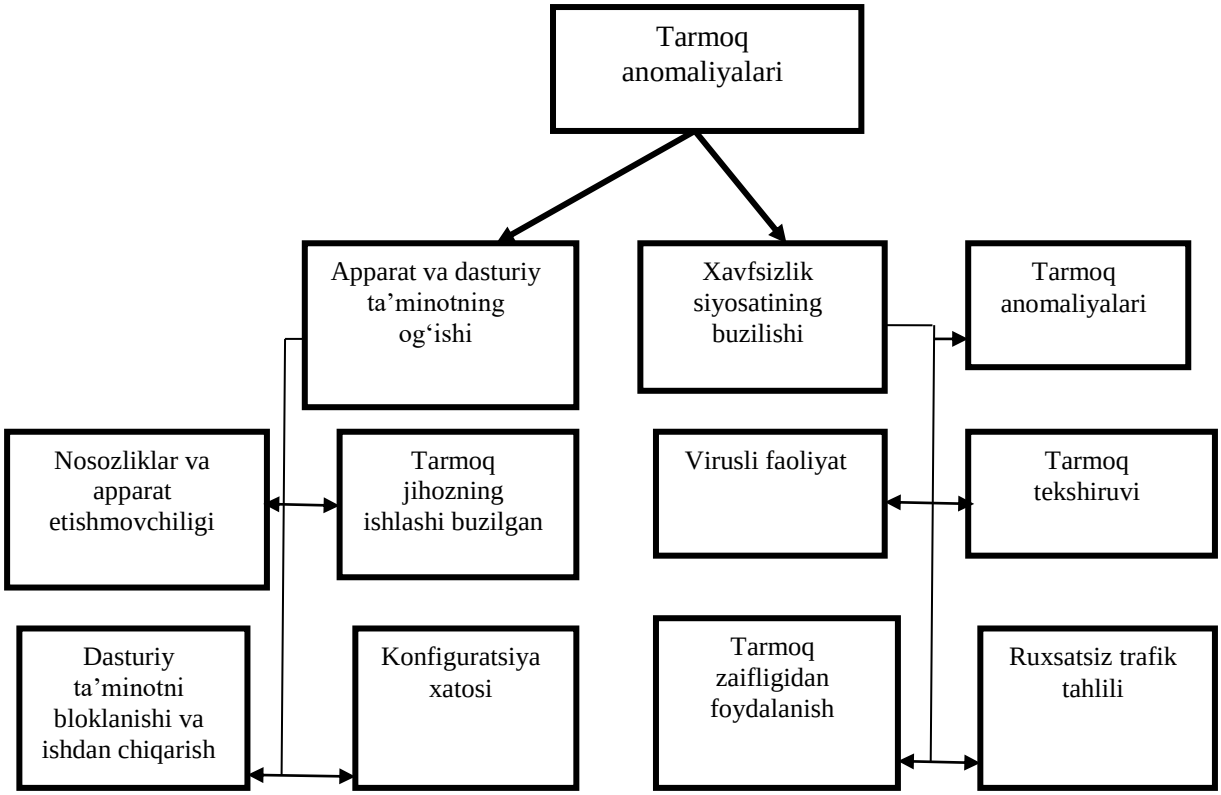
Rasmda keltirilgan tartibda tasniflanishi mumkin bo‘lgan tarmoq anomallarining paydo bo‘lishining turli sabablari bor.

Tarmoqlarida ma’lumotlar oqimlaring samarali taqsimlanishini va ularni tugunlar o‘rtasida trafiklarni kechikishini extimoyiligini optimallashtirish bilan xavfsiz ishlashni amalga oshirish uchun tarmoq anomallarini aniqlashning ko‘plab usullari va tartiblari ishlab chiqilgan.

Hujumlarni aniqlashning quyidagi asosiy usullari:

“imzolarni tahlil qilish;
statistik tahlil;
yaxlitlikni boshqarish;
davlat tizimlarini tahlil qilish;
hujum ssenariylarining jadvali;
ekspert tizimlar;
texnik xususiyatlarga asoslangan usullar;

neyron tarmoqlar;
immunitet tarmoqlar;
klaster tahlili;
xulqiy biometriya;
sikl tahlili [1].



1-rasm. Tarmoq anomaliyalari sabablarining tasnifi.

Tadqiqot usullari. Hisoblab, tarmoqlarida ma'lumotlar oqimlaring samarali taqsimlanishini va tugunlar o'rtasida trafiklarni kechikishini extimoyiligini optimallashtirish hamda imzolarni tahlil qilish yordamida anomallarni aniqlash usuli hisoblash tarmog'iga kirishni aniqlash uchun ishlatilgan birinchi usullardan xisoblanadi. Usulning prinsipi tizimning hozirgi holatini va unda bajarilgan amallarni xarakatlarini o'zaro taqqoslash - oldindan tuzilgan ma'lumotlar bazasida saqlangan holda. [1]

Bunday holda viruslar yoki hujumlar haqida ma'lumot saqlanadi, ya'ni bunda ma'lumotlar to'plami (yoki lug'atlar) tushuniladi. Ushbu lug'atlarga kirishda shubhali fayl (paket) lug'atdagi ma'lumotlar bilan taqqoslanadi (virus hujumi haqida ma'lumot) va keyinchalik blokirovka qilish (karantinga yuborish) yoki ushbu namunaga (paketga) ruxsat berish to'g'risida qaror qabul qilinadi. Imzolar bilan ishlashning yaqqol namunasi antivirus dasturlari va fayllarni yoki paketlarni ko'rib chiqish orqali, dastur mualliflari tomonidan tuzilgan ma'lum viruslarning lug'atiga murojaat qiladigan antivirus dasturlari tushuniladi.

Ushbu usulning afzalliklari quyidagilarni o'z ichiga oladi: tahlil tezligi; oldindan tuzilgan, xususan ishni soddalashtiradigan qoidalar ro'yxati (ya'ni qoidalarni yozish, tushunish, sozlash) tushuniladi. Bu yerda kamchiliklar ko'p bo'lsa sonli qoidalar (imzolar) to'planishi tufayli vaqt o'tishi bilan tezlikning pasayishi; noma'lum hujumlardan himoya etaolmasligi ham mumkin.

Statistik tahlil usuli tizim shablonidan uzoqlashganda hujumni aniqlashga asoslanadi. Tizimning normal ishlashini o'z ichiga olgan oldindan belgilangan parametrlar bilan shablon (sozlamalar bilan fayllar to'plami) yaratiladi. Doimiy ravishda tarmoq trafigining ba'zi parametrlari o'lchanadi, masalan, TCP (Transmission Control Protocol) va UPD (User Datagram Protocol)

paketlarining soni. Olingan seriyalar tarmoqning "normal" harakatlarini aks ettiradi deb taxmin qilish mumkin. Keyinchalik, hozirgi holatni "normal" xatti-harakatlardan og‘ishini bilish uchun qidiruv o‘tkaziladi. [1]

Usulning afzalligi moslashuvchanlik (noma’lum hujumlarni aniqlash qobiliyati), ahvolga tushib qolish - bu obyekt faoliyatidagi o‘zgarishlarni aniqlay olmaslik (natijada o‘tkazib yuborilgan hujumlar) tushuniladi.

Hozirgi vaqtda «normal» holat bilan taqqoslash uchun yetarli miqdordagi algoritmlar ishlab chiqilgan. Ammo eng samarali va tez-tez ishlatiladiganlardan biri bu Holt-Winters usuli.

Birinchidan, ushbu usul – RRD tool (dastur) xisoblanadi, u RRD (Round–robin Database) dasturi bilan ishlash imkoniga ega. RRD dasturi ma’lumotlar bazasida (RRD) saqlanadigan ma’lumotlarga asoslanib ma’lumotlar jadvalini tuzish imkoniga ega. Ikkinchidan, bu usul allaqachon amalda isbotlangan.

Holt-Winters bashorat qilish usuli kuzatilgan vaqt seriyalarni (tarmoq trafigi ma’lumotlari) uch qismga ajratish mumkinligiga asoslanadi, bular: normal komponent, chiziqli og‘ish va mavsumiy og‘ish. Ushbu tarkibiy qismlarning har biri vaqt o‘tishi bilan o‘zgaradi va uning o‘zgarishini ekspansional tekislash (vaqt seriyasini tekislash usuli, natijada yanada aniq prognozlash) yordamida topish imkoniga ega bo‘ladi. [1]

Tahlil qilish usulidan foydalanganda ish jarayoni ular orasidagi o‘tish holati sifatida tavsiflanadi. Natijada, butun tizim yo‘naltirilgan grafik yordamida amalga oshiriladi, odatda cheksiz ko‘p sonli vertikalar mavjud bo‘ladi. Natijada muayyan yaroqsiz yo‘llarning himoyalangan tizimi jadvaldagi qidirishni tahlil qiladi. Ushbu holat olib keladigan o‘tish ketma-ketligini aniqlash hujumni muvaffaqiyatli aniqlashni anglatadi.

Usulning afzalligi uning tekshirilishi va kamchiliklari qatorning qisman mos kelishi bilan hujumlarni aniqlashning iloji yo‘qligida bo‘ladi.

Hujum ssenariylarini grafik usuli - bu tizimning to‘g‘riligining ma’lum bir xususiyatiga asoslanib, barcha ma’lum bo‘lgan hujum ssenariylarini o‘z ichiga olgan grafik tuzilishidir. Ushbu xususiyat asosida tizimning xatti-harakati ruxsat etilgan va qabul qilinmaydigan bo‘ladi. Ushbu usuldan foydalanib, ma’lum bir himoyalangan tizim uchun nomaqbul xatti-harakatlarning barcha variantlari to‘plami qurilgan bo‘lib, u hujumning mumkin bo‘lgan yo‘llarini tavsiflaydi. [1] Ushbu usul tizimlarni loyihalashda zaifliklarni qidirish uchun amalga oshirilishi mumkin, ammo yuqori hisoblash murakkabligi tufayli hujumlarni aniqlash vazifasi uchun qo‘llanilmaydi. Usulning afzalliklari moslashuvchanlik va tekshirish qobiliyatidir, ahvolga tushib qolish esa hisob-kitoblarning yuqori darajada murakkabligi.

Ekspert tizimli usul tizimni faktlar va ta’sir ko‘rsatuvchi qoidalar ko‘rinishida tavsiflashga asoslangan. [1] Kirishda tizim tizimda kuzatilgan hodisalar haqida ma’lumot beradi. Faktlar va qoidalarga asoslanib, tizim hujumning mavjudligi to‘g‘risida xulosa chiqaradi. Ushbu usul uchun ko‘p sonli alternativalarning to‘liq ro‘yxatlanishi kuzatilishi mumkin. Ekspert tizimlardan foydalanishning afzalligi paydo bo‘lgan muammolarning sabablari va yechimlarini ajratish qobiliyatidadur. Bu yerda kamchiliklarga katta hajmli ma’lumotlar bilan ishlashda past samaradorlik va baholash parametrlari tabiatiga bog‘liqlikni hisobga olish qiyinligi kiradi.

Neyron tizimli usuli himoyalangan tizimlarning ma’lum bir sonli fazoda traektoriya shaklida ifodalanishiga asoslangan. [1] Hujumlarni aniqlash vazifasi naqshni aniqlash vazifasi sifatida ko‘rib chiqiladi. Usulning afzalligi shundaki, u нисбатан паст ҳисоблаш murakkabligiga ega va moslashishi mumkin. Usulning kamchiliklari uning tekshirilgan tarmoqda faqat tekshirib bo‘lmaganligi va beqarorligi sifatida ko‘rib chiqilishi mumkin.

Immun tizimli usul - tirik organizmning immunitet tizimi bilan o‘xshashlikka asoslanadi. [1] Buning afzalliklari allaqachon ma’lum bo‘lgan hujumlarga va usulning moslashuvchanligiga "antikorlarni" tezda olish qobiliyatiga ega bo‘ladi. Kamchiliklari hisoblashning murakkabligi va yana, tekshiri iloji mavjud bo‘lmaganligida.

Taqdim etilgan har bir usulni tahlil qilsak, shuni aytishimiz mumkinki, hozirgi vaqtda anomallarni bashorat qilishning eng samarali va aniq usuli statistik tahlildan foydalangan usul hisoblanadi. Taqdim etilgan har bir usul o‘zining afzalliklari va kamchiliklariga ega, bular, aniq tizimni tanlash va anomallarni aniqlashning tegishli usuli bo‘lib, u tashkilot budjetiga ta’siriga va xavfsizlik bo‘yicha mutaxassisning bilim darajasiga bog‘liqdur. Ushbu holatni amaliy qo‘llashda aniqlash funksiyalarini bajaradigan qurilmalar yoki dasturlarni ko‘paytirish tavsiya etiladi.

Bugungi kunga kelib, anomallarni aniqlash uchun ishlatiladigan eng keng tarqalgan vositalardan biri hujumlarni aniqlash vositalaridir. [2,3] Ushbu vositalar hisoblash yoki tarmoq resurslariga yo‘naltirilgan shubhali (g‘ayritabiiy) faoliyatni aniqlaydi va unga javob beradi. Biroq, mavjud hujumlarni aniqlash vositalarining hech biri hisoblash tizimlari trafikidagi g‘ayritabiiy faoliyatni to‘liq aniqlay olmaydi. Statistikaga ko‘ra, taxminan 80% qoidabuzarlik ichki tartibbuzarlar tomonidan amalga oshiriladi, ya’ni. tashkilot xodimlari orqali. [4]

Amaldagi hujumlarni aniqlash vositalari ichki hujumchilar tomonidan salbiy ta’sirlarni aniqlashda samarasiz. Zamonaviy hujumlarni aniqlash vositasi mavjud kamchiliklar bilan bog‘liq holda, anomaliyalar tarmog‘ini aniqlashning yangi usullarini ishlab chiqish va anomaliyaning kattaligini aniqlash va baholash, shuningdek uni bartaraf etish zarurligi to‘g‘risida qaror qabul qilish imkoniga ega.

Anomaliyalarni aniqlashga asoslangan harakatni boshqarishning umumiy sxemasi quyidagi funksional bloklar ko‘rinishida taqdim etilishi mumkin:

“tarmoq paketlari to‘g‘risida ma’lumot olish;

prognozni tuzish;

anomaliyalarni izlash va baholash;

anomaliyaga javob;

normativ-huquqiy bazani to‘ldirish va tahrirlash” [4].

Birinchi bosqichda prognoz qilish uchun zarur bo‘lgan barcha ma’lumotlar olinadi. Tarmoq yuklanishidagi mavjud ma’lumotlarga asoslanib prognoz qilishning asosiy maqsadi kelajakda ma’lum vaqt davomida trafik hajmining qiymatini olishdir, shuning uchun IP paketi sarlavhasidan paketning umumiy uzunligi to‘g‘risida ma’lumot olish, shuningdek paketni qabul qilish sanasi va vaqtini saqlash kerak. Filtrlashda IP -paketning manzili va manzil manzili to‘g‘risidagi ma’lumotlardan foydalanish mumkin. Shunday qilib, IP - paketdan trafikni bashorat qilish uchun quyidagi ma’lumotlar olinadi:

IP -paket hajmi;

manzili IP -manzili;

belgilangan IP -manzil;

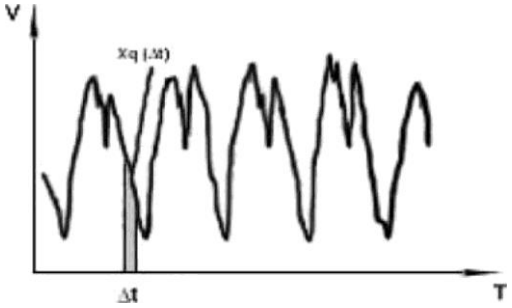
IP -paketning qabul qilingan sanasi;

IP -paketni qabul qilish vaqti [4].

Shuni yodda tutish kerakki, tarmoqdagi trafikni prognozlash to‘plangan statistikaga asoslanadi.

Quyida vaqt ketma-ketligini tahlil qilgan asosida trafikni taxmin qilish algoritmini taqdim etish mumkin.

1. Ma’lumotlarni tanlash. Birinchi bosqichda bashorat qilish amalga oshiriladigan ma’lumotlarning shakli va miqdorini aniqlash kerak bo‘ladi. Siklik tahlil ma’lumotlarning bir xilligiga bog‘liqdir. Amaldagi ma’lumotlar bir hil tuzilishga ega bo‘lishi kerak, aks holda tahlildagi Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlari sikllarning tuzilishini o‘zgartirishi mumkin. Shunday qilib, anomallarni qidirish va baholashda kompyuter tarmog‘ining keskin o‘zgarishini (masalan, ko‘p sonli xostlarni ulash yoki jadvalni o‘zgartirish), siklning shaklini o‘zgartirishi mumkin. Sikl tahlili bir qator ma’lumotlar bilan ishlashni o‘z ichiga olganligi sababli, vaqt o‘tishi bilan trafik hajmining o‘zgarishini tavsiflaydigan bir qator qiymatlar ko‘rinishida tarmoq trafigi bo‘yicha mavjud ma’lumotlarni yaratish mumkin. Buning uchun transport oqimini ajratib ko‘rsatish kerak bo‘ladi (2-rasm).



2-rasm. Jadvalni diskretlashtirish.

2-rasmda tarmoq trafigi oqimini aks ettiruvchi grafik ko‘rsatilgan: t - vaqt absissasi, v - trafik hajmi ordinatasi o‘qga chizilgan holatda. T - vaqt ichida trafik statistikasi to‘plangan holda ko‘rsatilgan bo‘lsa agar, shunda biz qo‘yidagi ma’lumotlarni olishimiz mumkin:

$$Q = \frac{T}{\Delta t} \quad (1)$$

Keyinchalik, har bir interval uchun ushbu vaqt oralig‘iga to‘g‘ri keladigan tarmoq paketlari qo‘shiladi:

$$X_q(\Delta t) = \sum_{j=1}^{R} V_{\text{пкетллар}} \ , \ (2)$$

bu erda R - oraliqqa tushgan tarmoq paketlarining soni; Δt ; Q - intervalning soni; $Q = 1, \ldots Q$, X_q - vaqt o‘tishi bilan trafik hajmining o‘zgarishini tavsiflovchi, tanlab olish chastotasi bilan tavsiflangan bir qator ma’lumotlar.

2. Ma’lumotni tekislash. Ma’lumot to‘g‘risida qaror qabul qilgandan so‘ng, tasodifiy o‘zgarishini istisno qilish kerak. Buning uchun ma’lumotlarni tekislash sari qadam qo‘yiladi. Tasodifiy tebranishlarni bartaraf etish uchun qisqa muddatli markazlashtirilgan harakatlanuvchi o‘rtacha ma’lumotlar seriyasidan foydalanish mumkin.

3. Mumkin bo‘lgan sikllarni qidirish. Tasodifiy tebranishlarni yo‘q qilib, sikllarni to‘g‘ridan-to‘g‘ri qidirishga o‘tish mumkin. Ko‘rib chiqilayotgan qatorlarning chastota tarkibiy qismlarini aniqlash uchun spektral tahlil usulidan foydalanish kerak bo‘ladi. Spektral tahlilning matematik asosi Fyurening o‘zgarishi deyaladi. Tarmoq trafikining qayta ishlangan statistikasi raqamli seriyali shaklga ega bo‘lganligi sababli, diskret Furye o‘zgartirish usuli chastota tarkibiy qismlarini aniqlash uchun mos keladi. Biz quvvat spektrini qo‘yidagicha grafik tarzda tasvirlanadi. Siqilish yuqori bo‘lgan joylarda cho‘qqilar mumkin bo‘lgan sikllarni ko‘rsatadi. Axborot oqimlarining sikl chastotasining qiymati quvvat spektrining yuqori qiymati kuzatiladigan indeks bo‘ladi. Mumkin bo‘lgan sikllarni va ularning chastotalarini aniqlab, biz odatdagi (haqiqiy) amplituda A va fazani hisoblaymiz.

b chastotasi topilgan bo‘lsa, unda *S* ni tashkil etadigan mumkin bo‘lgan sikllarni aniqlashimiz kerak bo‘ladi, ya’ni har bir chastota qiymati yuqori spektral qiymatlarning to‘planish mintaqasida *S* to‘plamining elementi hisoblanadi. Keyin siklni tavsiflovchi funksiya quyidagicha tariflanadi:

$$f_h(t) = A_h \cos(S_h t + \varphi_h), \quad (3)$$

Biroq, yuqorida aytib o‘tilganidek, quvvat spektrining yuqori qiymati faqat sikl mavjudligini taxmin qiladi. Shuning uchun, keyingi qadam topilgan sikllarni tasdiqlash kerak bo‘ladi. Buning uchun ma’lum miqdordagi mezonlarni tekshiri lozim.

1. Trafikdagi tendensiya tarkibiy qismlarini olib tashlanganda, tekshirish sikllarining statistik ishonchliligi sifati baholanadi, bu yerda ma’lumotlarning to‘g‘ridan-to‘g‘ri mavjudligiga bog‘liqligini inobatga olish kerak bo‘ladi. Shuning uchun, tekshirishdan oldin, tendensiyani ma’lumotlardan olib tashlash lozim. Buning uchun harakatlanuvchi o‘rtacha qiymatdan og‘ish usuli qo‘llaniladi.

Bu holda, harakatlanuvchi o‘rtacha ma’lumotlardagi o‘sish kuchlarini aks ettirish mumkin, shuning uchun uni ma’lumotlardan ajratib olishda tarkibiy qismini olib tashlash kerak. Shunday qilib, ma’lumotlardagi tendensiyani olib tashlash uchun har bir topilgan chastota uchun tekislash nuqtalari soni bilan bir qator ma’lumotlarning harakatlanuvchi o‘rtacha qiymatini hisoblash lozim. Ma’lumotlardagi o‘sish kuchlarini olib tashlaganimizdan so‘ng, biz topilgan sikllarni statistik ahamiyatga ega ekanligini tekshirishni boshlashimiz mumkin.

2. Statistik ahamiyatga ega bo‘lgan sikllarni tekshirish uchun *F*-koeffitsiyenti va xi-kvadrat testlari odatda sikllarni baholash uchun ishlatiladi, shuning uchun uni tarmoq trafikida sikllarni sinash uchun ham ishlatish mumkin. E’tibor bersak, test natijalari ma’lumotlardagi siklni takrorlash soniga bog‘liq bo‘ladi. Bu kabi takrorlashlar qanchalik ko‘p bo‘lsa, ushbu sikl shunchalik muhimdir. Kelajakda sikllarni birlashtirish va loyihalash mumkin.

3. Trafikni bashorat qilish, odatda sikllarni birlashtirish va loyihalash bosqichida sodir bo‘ladi. Buning uchun sikllar birlashtirilib, olingan natijaga asoslanib, kelajakda ularning xatti-harakatlarini taxmin qilish mumkin. Proeksiyalash uchun sikllar matematik ravishda bitta umumiy egri chiziqga birlashtiriladi.

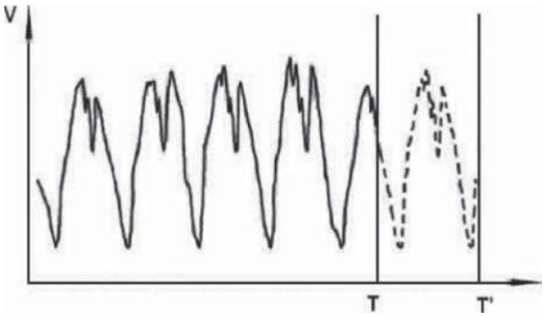
Sinovlar *D* siklidan o‘tdi deb taxmin qilsak. Tasdiqlangan axborot oqimlarining sikllar bir qator ma’lumotlarning chastotasini tavsiflovchi umumiy egri holatda chizilishi mumkin, masalan:

$$\overline{V}(t) = \sum_{j=1}^{D} f_h(t) \qquad (4)$$

Ushbu funksiya T vaqtidagi ma’lumotlar asosida topilgan trafik chastotasini tavsiflaydi, natijada kelajakka ekstrapolyatsiya qilinishi mumkin va bu T vaqt uchun trafikning taxmin qilingan qiymatini ko‘rsatadi (4-rasm):

$$V_{\text{bashoratlash}}(t) = \sum_{j=1}^{D} f_h(t)\,, \qquad (5)$$

Haqiqiy vaqtda keladigan trafik miqdorini aniqlash uchun tarmoq paketlari to‘g‘risida olingan ma’lumotlarni ishlatish kerak.



3-rasm. Trafikni bashorat qilish

Keyinchalik olingan trafikdagi ma’lumotlarga asoslanib va hozirgi prognozga tayangan holda anomaliya haqida ma’lumot yoziladi. Agar anomaliya topilgan bo‘lsa, anomaliya izlash natijasi anomaliya manbaini izlash blokiga uzatiladi. Anomaliyalar manbalarini aniqlash anomaliyalarni qidirish natijalariga va real vaqtda kelib tushadigan tarmoq paketlari to‘g‘risidagi ma’lumotlarga asoslanadi. Keyinchalik, anomaliyaning kattaligi taxmin qilinadi. Baholashda qoida buzarlar haqida olingan ma’lumotlar, paketlar to‘g‘risidagi ma’lumotlar, shuningdek ekspertning taxliliga asoslangan holda qaror qabul qiluvchi o‘zi baxo beradi[5]. Anomaliyaning kattaligi haqida ma’lumot umumlashtirilib, kelajakda foydalanish uchun uzatiladi.

Tarmoq trafigi miqdoridagi anomaliyalarni qidirishda quyidagi xususiyatlardan foydalanish kerak.

haqiqiy trafikning taxmin qilinganidan chetga chiqish darajasi;

haqiqiy trafikni tekislash uchun oynaning o‘lchamlari;

IP - manzil tarmog‘i va niqob;

transport yo‘nalishi (kirish yoki chiqish);
tashqi yoki ichki tarmoq [4].

Xulosa qilib shuni ta’kidlash kerakki, Mudofaa vazirligi telekommunikatsiya tarmoqlarini vaqt ketma-ketligini tahlil qilish asosida ko‘rib chiqilayotgan trafikni prognozlash algoritmi tarmoq trafigini davriy ravishda qidirish asosida tarmoq yuklamalarini aniqlashga imkon beradi. Ushbu metodologiyani qo‘llash natijasida olingan ma’lumotlar Mudofaa vazirligi telekommunikatsiya tarmoq uskunalarida nosozliklarni bartaraf etish, dasturiy konfiguratsiyadagi xatolarni aniqlash, foydalanuvchilarning tasodifiy va qasddan qilingan xatti-harakatlarini, shuningdek tajovuzkorlarning xatti-harakatlarini aniqlash uchun ishlatilishi mumkin. Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarini integrallashgan boshqarish tizimlaridagi axborotni majmuaviy kriptografik himoya qilish algoritmlari taklif qilindi. Olingan algoritmlar boshqaruvchi ma’lumotlar bilan ruxsatsiz tanishib chiqish imkoniyatini aniqlash va buning oldini olish va aloqa kanallari bo‘yicha axborot uzatish jarayonlarini himoya qilish imkoniyatini beradi. Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining vaqt ketma-ketligini tahlil qilish asosida trafikni prognoz qilishning matematik modeli yaratildi va bu o‘z o‘rnida tarmoq yukini davriylikni qidirish asosida tarmoq yukini aniqlashga imkon beradi.

Mudofaa vazirligi telekommunikatsiya tarmoqlarida axborot oqimlarini qayta ishlashni taqsimlash vazifasini extimoligini aniqlab va qayd etilgan axborot xavfsizligini ta’minlash muammoli vazifani algoritmini belgilashda qabul qilib telekommunikatsiya tarmoqlarini ish samaradorligini oshishiga olib keladidigan omillar aniqlangan: protokllarni sozlash, axborot bloklarinng kolliziyasi, axborotlarni uzatishda qo‘llanilayotgan xatolarni aniqlash va to‘g‘rilash uslublari turi, axborot kadrlarining uzunligi va boshqalar.

Anomaliyaning mavjudligi to‘g‘risida qaror qabul qilish uchun qo‘llab-quvvatlash tizimi ishlab chiqilgan bo‘lib, uning asosida anomaliyaning kattaligini baholash va uni yo‘q qilish uchun nazorat choralarini ko‘rish zarurligi to‘g‘risida qaror qabul qilish lozim. Mudofaa vazirligi telekommunikatsiya tarmoqlarida uzatilayotgan axborot oqimlarining tuzilgan modelga asoslangan ma’lumotlarni boshqarish uslubi ishlab chiqilgan bo‘lib, bu Mudofaa vazirligi telekommunikatsiya tarmoqlarida ma’lumotlarni uzatish samaradorligini oshirishga imkon beradi, chunki bu nafaqat hisoblash tarmog‘idagi g‘ayritabiiy trafikni aniqlash, balki anomaliyani sonli baholash va uni yo‘q qilish choralarini ko‘rish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Yemelyanov V.N., Yemelyanova M.M., Zinovyeva YE.L., Shamanov M.Y. Analiz metodov obnarujeniya anomaliy setevogo trafika / V sbornike: Priborostroyeniye v XXI veke - 2015. Integratsiya nauki, obrazovaniya i proizvodstva Sbornik materialov XI Mejdunarodnoy nauchno-texnicheskoy konferensii. 2016. S. 420-425.
2. Belyayev A., Petrenko S. Sistemi obnarujeniya anomaliy: noviye idei v zashite informatsii [Elektronniy resurs] // Cit Forum [Sayt]. URL: http://citforum.ru/security/articles/anomalis/ (data obrasheniya: 14.03.2018).
3. Mikova S.Y., Oladko V.S. Model sistemi obnarujeniya anomaliy setevogo trafika // Informatsionniye sistemi i texnologii. 2016. №5 (97). S. 115-121.
4. Ajmuxamedov I.M., Maryenkov A.N. Poisk i otsenka anomaliy setevogo trafika na osnove siklicheskogo analiza // Injenerniy vestnik Dona. 2012. T. 20. № 2. S. 17-26.
5. Izbosarov, A.F. Mudofaa vazirligi qo‘shinlar boshqaruvini raqamlashtirish asosida Qurolli kuchlar kuch tuzilmalari o‘rtasida yagona himoyalangan axborot kommunikatsiya tizimini joriy etish / A.F.Izbosarov // O‘R MV AKT va AHI ilmiy-amaliy konferensiyasi maqolalar. – 2022. – 1-sho‘ba. B. 4-7.
6. Izbosarov, A.F. Mudofaa vazirligi qo‘shinlarida maxsus mobil (dala) axborot kommunikatsiya mashinalarini raqamlashtirish asosida majmuasini ishlab chiqish / A.F.Izbosarov // “Harbiy aloqa va AKT xabarlari” ilmiy-uslubiy jurnalida – 2021. –№2(6). B. 32-39.